IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 5, May 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Image Steganography Applications for Secure Communications

Dr.M.N.Nachappa[1], Vignesh Kamble R P [2].

Professor and Head, School of CS and IT, Jain University, Bangalore[1].
2. Graduate Student, Master of computer application, Jain University, Bangalore[2].
Email:mnnachappa@gmail.com[1], vigneshkamble@gmail.com[2].

***Abstract*— In the present age, the exploration of digital multimedia content has lead to it being utilized as a medium of safe and secure communication. The art of secret communication by a secret medium like images is known as steganography as the rival method of detecting the presence of embedded data in media is called steganalysis. In this review article we have studied and analyzed the different methodologies from various researchers in their research. The main goal of image steganography is to hide the existence of the data message from illegal intention. Image steganography proposes a job to transfer the embedded secure data to the target destination without being detected through the unauthorized user. Various carrier file formats would be used, but digital images are large enough used due to the frequency and huge users on the worldwide Internet. To hide the secret data in images, there are large ranges of steganographic methodologies exist some are complex in used than others method. Every method has respective strong and weak points.**

Keywords— Steganography ,Image Steganography, stego image , Steganalysis , Secure Communication.

1. INTRODUCTION

The word steganography is derived from the Greek words stegos meaning cover and graphy meaning writing defining it as covered writing. Image steganography the information is hidden exclusively in images.
Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The actual files can be referred
to as cover text, the cover image, or cover audio message. After inserting the secret message, it is referred to as stego medium.
A stego-key has been used for hiding encoding process to restrict detection or extraction of the embedded data.
Communication of secret information is a critical factor in information technology that continues to create challenges with increasing levels of sophistication. When communication takes place between parties that are located on the same secure network, these challenges can be considered as manageable. However, in the modern era expectations are that one can travel the world and receive secret information at the same time without jeopardizing the confidentiality of secret information. In these situations where the involved parties are spatially separate, the security of secret information cannot rely only on the advanced technologies of secure networks, and additional security mechanisms should be incorporated.

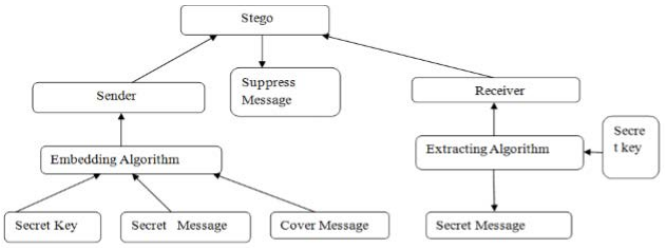

Fig:1.1 Steganography

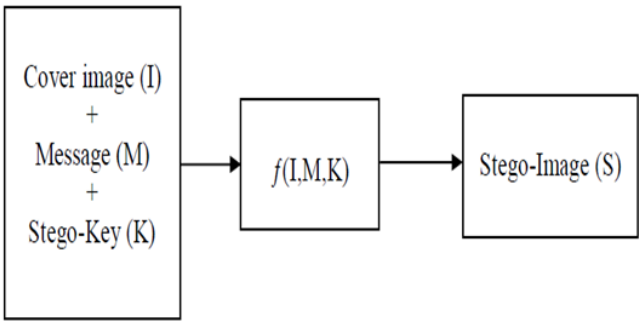

Fig:1.2 Simple Steganography Model

Applications of Steganography

(a) Secret Communications the use steganography does not advertise secret communication and therefore avoids scrutiny of the sender side, message, and recipient. A secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.
(b) Feature Tagging Elements can be embedded inside an image, as the names of individuals in a photo or locations in a map. Copy the stego-image also copies all of the embedded features and only parties who possess

the decoding stego-key will be able to extract and view the features.

(c) Copyright Protection Copy protection mechanisms that prevent data, generally digital data, from being copied.

2. SYSTEM MODULE

Steganography hide the messages inside the Cover medium, Many Carrier formats. Breaking of steganography is known as Steganalysis.

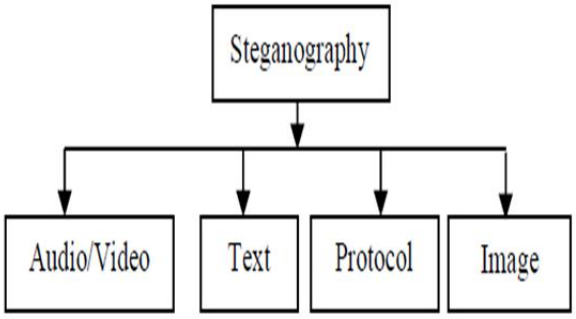

Fig:1.3 Categories of Steganography

The insertion and analysis of water-marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

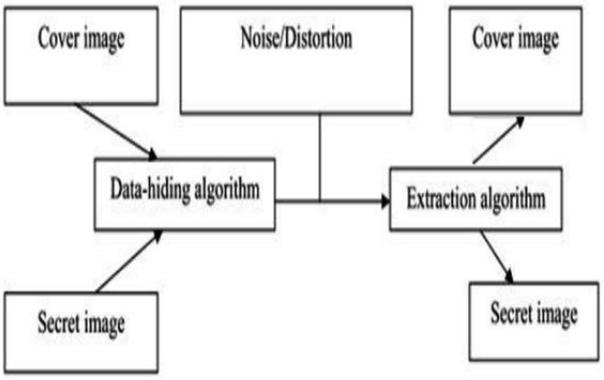

Fig:1.4 Image Steganography

Image Steganalysis

Steganalysis is the breaking of steganography and is the science of detecting hidden information. The major objective of steganalysis is to break steganography and the detection of stego image. All steganalysis algorithms depend on steganographic algorithms introducing statistical differences between cover and stego image.

Steganalysis types:

Visual attacks it discovered the hidden information, that helps to separate the image into bit planes for further more analysis. The statistical attacks Statistical attacks may be passive or active. Passive attacks include identifying presence or absence of a secret message or embedding algorithm used. Active attacks are used to investigate embedded message length or hidden message location or secret key used in embedding. Structural attacks the format of the data files changes as the data to be hidden has been embedded, identifying this characteristic structure changes can help us to find the presence of image/text file.

Various Methods of Image Steganography

(a) Data Hiding Method: hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the existence of a message by hiding information into various carriers. This prevents the detection of hidden information.

(b) Data Embedding Method: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes.

(c) Data Extracting Method: It is used to retrieve an original message from the image; a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with the decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, the unzip the text file and transfer the secret message from the text file to retrieve the original secret message.

Features of Image Steganography

(a) Transparency: The steganography should not affect the quality of the original image after steganography.

(b) Robustness: Steganography could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction, steganography should be robust against variety of such attacks.

(c) Data payload or capacity: This property describes how much data should be embedded as a steganography to successfully detect during extraction.

Secure Communications

In the context of this dissertation, secure communication is defined as sending and receiving information with the certainty that the information remains safe and protected against attacks.

1. The fact that secret information is being communicated should be concealed and communication should take place in an inconspicuous manner.
2. The confidentiality of secret information should be ensured, even under the suspicion that secret information

is being communicated.
3. The communication should allow the user to comply with international laws regarding the use of cryptography.
4. The communication should be done (almost) as easily as it would have been using traditional secure communication systems and should be convenient to use by nontechnical users.

3. LITERATURE REVIEW

In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional.
Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key. The order parameter of this transform.
In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit- inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality.
In the year of 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. Investigated on Medical records are extremely sensitive patient information a multi secure and robustness of medical image based steganography scheme is proposed. This methodology provides an efficient and storage security mechanism for the protection of digital medical images. Authors proposed a viable steganography method using Integer Wavelet Transform to protect the MRI medical image into a single container image. The patient's medical diagnosis image has been taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In this case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. It has been observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms.
In the year of 2012 Thenmozhi, S. and Chandrasekaran, M., presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.
In the year of 2012 Das, R. and Tuithung, T. proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of Huffman encoded bit stream and Huffman Table are also
embedded inside the cover image, in order that the Stego-Image becomes standalone information to the receiver. Results show that the algorithm has a high capacity and a good invisibility. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches. The satisfactory security is maintained in this research.
In the year of 2012 Hemalatha, S, Acharya, U.D. and Renuka presented integer Wavelet Transform (IWT) is used to hide the key thus it is very secure and robust because no one can realize the hidden information and it cannot be lost due to noise or any signal processing operations. Result shows very good Peak Signal to Noise Ratio, which is a measure of security. In this method the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands. In the 2012 Reddy, H.S.M., Sathisha, N. and Kumari, A.
worked on the steganography is used to hide. Secure Steganography using Hybrid Domain Technique (SSHDT). The cover image of different formats and sizes are considered and resized to dimensions of power of 2. The Daubechies Lifting Wavelet Transforms (LWT) is applied on cover image to generate four sub bands XA, XH, XV and XD. The XD band is considered and divided into two equal blocks say upper and lower for payload embedding. The payload of different formats are considered and resized to dimensions of power of 2. The payload is fragmented into four equal blocks. The Decision Factor Based Manipulation (DFBM) is used to scramble further stego object to improve security to the payload. Dubechies Inverse LWT (ILWT) is applied on XA, XH, XV and XD stego objects to obtain stego image in spatial domain. It has been observed that PSNR and embedding capacity of the proposed algorithm is better compared to the existing algorithm.

4. MOTIVATION

In steganography, the message is embedded into the digital media rather than encrypting it. The digital media contents, called the cover, can be determined by anybody, the message hidden in the cover can be detected by the one having the true key. The message in the message after the receiver gets the data. That allows steganography to protect

the embedded information after it is decrypted. Steganography is therefore broader than cryptography.
Signal processing area includes- filtering, de-noising method, interference suppression, radar signal processing, electromagnetic wave propagation, and wireless communication systems. The area of the image processing applications includes steganography, watermarking

5. CONCLUSION

We have studied for improving the steganalysis performance and also analyzing the hiding capacities of the existing research work. The steganalysis performance of state-of-the-art detectors is near-perfect against current steganographic schemes. A novel, robust and secure hiding schemes that can resist steganalytic detection must be implemented. Hiding schemes are characterized by three complementary requirements- security against steganalysis, robustness beside distortions in the transmission channel, and capacity in terms of the embedded method. This work would be able to be extended for different formats of images. This work may be extended using other transforms methods also.
Although there are many advantages of the internet, it has also opened a new way for invasion of our privacy and intellectual property by hackers and unauthorized users. Many techniques have been invented since these problems appeared. One useful technique to protect information via the internet is steganography. Digital watermarking is one of the popular applications for steganography. Users can hide important information within an image by using an invisible watermark when they transmit data.

REFERENCES

[1]. Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on* , vol., no., pp.97,100, 1-2 March 2013.
[2]. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on* , vol., no., pp.385,390, 27-29 Sept. 2013.
[3]. Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on* , vol., no., pp.14,18, 30-31 March 2012.
[4]. Hemalatha, S.; Acharya, U.D.; Renuka, A.; Kamath, P.R., "A secure image steganography technique using Integer Wavelet Transform," *Information and Communication Technologies (WICT), 2012 World Congress on* , vol., no., pp.755,758, Oct. 30 2012-Nov. 2 2012.
[5]. Amat, P., Puech, W., Druon, S., & Pedeboy, J. P. (2010). Lossless 3D steganography based on MST and connectivity modification. Signal Processing: Image Communication, 25(6), 400-412. doi: 10.1016/j.image.2010.05.002
[6]. Babu, K. S., Raja, K. B., Kiran, K. K., Manjula Devi, T. H., Venugopal, K. R., & Patnaik, L. M. (2008, 19-21 Nov. 2008). Authentication of secret information in image Steganography. Paper presented at the TENCON 2008 - 2008 IEEE Region 10 Conference
[7]. Awwad, W. F., Mansour, R. F., & Mohammed, A. A. (2012). A robust method to detect hidden data from digital images. [Report]. Journal of Information Security, 3(2),
[8]. Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," *Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on* , vol., no., pp.1188,1193, 20-21 March 2013.
[9]. Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," *Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on* , vol., no., pp.1,5, 18-20 Dec. 2012.
[10]. Reddy, H.S.M.; Sathisha, N.; Kumari, A.; Raja, K.B., "Secure steganography using hybrid domain technique," *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on* , vol., no., pp.1,11, 26-28 July 2012.
[11]. Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I., "A new approach for LSB based image steganography using secret key," *Computer and Information Technology (ICCIT), 2011 14th International Conference on* , vol., no., pp.286,291, 22-24 Dec. 2011.
[12]. Keshari, S.; Modani, S.G., "Weighted fractional Fourier Transform based image Steganography," *Recent Trends in Information Systems (ReTIS), 2011 International Conference on* , vol., no., pp.214,217, 21-23 Dec. 2011